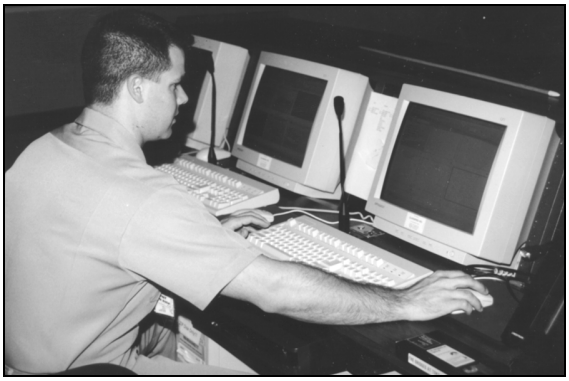
DEFENSE MESSAGE SYSTEM (DMS)



The Defense Message System (DMS) is designed to enable anyone in DoD to exchange messages with anyone else in DoD using a secure, accountable, and reliable writer-to-reader messaging system. DMS supports organizational and individual messaging, handling both unclassified and classified traffic. DMS is intended to reduce the cost and manpower demands of the legacy organizational messaging system based on 1960s technology—the Automatic Digital Network (AUTODIN). To replace AUTODIN, DMS must be implemented in more than 40,000 organizations at more than 700 sites worldwide and must support message exchanges with tactical forces, allies, other Federal Government users, and defense contractors. The DMS program will ensure innovation by employing the latest commercial technology, supporting Allied Communications Publications (ACP) 120, and operating on Defense Information Infrastructure computers and communications backbone. While today's security needs require using the international X.400 messaging standard and X.500 directory services standard, the DMS program expects to eventually move to the use of commercial Internet e-mail standards once they evolve to adequately support security and military features. The timeline for such evolution is unclear at this time, but is a number of years in the future.

BACKGROUND INFORMATION

The Defense Information Systems Agency began the DMS program in 1988. Since the 1997 IOT&E of release 1.0, DMS has continued to improve through OAs in 1998 and 1999, and an OT&E of release 2.1. The AUTODIN backbone has been downsized to three message-switching centers called DMS Transition Hubs (DTHs). An OA, conducted late October through early November 2000, found release 2.2 to be not effective and not suitable. The 2.2 OA revealed several system deficiencies, as well as numerous problems with site installations, configurations, and overall security posture of the system. DOT&E directed that DMS 2.2 be retested after the deficiencies were rectified.

TEST & EVALUATION ACTIVITY

A Limited Field Test (LFT) of DMS 2.2 was conducted from March 26 through April 3, 2001 to reassess system effectiveness problems identified during the earlier OA. The LFT did not address operational suitability. Subsequently, DMS 3.0 underwent an OA in November 2001, and is now scheduled for a full OT&E late spring 2002. This OT&E will determine operational effectiveness and

suitability for sensitive compartmented information enclaves as well as unclassified and secret traffic. It will also have users performing more realistic mission essential tasks in a scenario-like environment.

TEST & EVALUATION ASSESSMENT

DMS 2.2 performed significantly better in the LFT than in the earlier OA, and it was concluded that DMS 2.2 is operationally effective but not suitable. Administering DMS requires attention to detail and relies heavily on complex documentation and manual processes. Security tests revealed that system administrators had failed to protect all elements. A typical system administrator was poorly equipped to install, maintain, troubleshoot, and ensure security configuration of the system. In spite of these deficiencies, release 2.2 did not pose sufficient risk at this point in DMS maturation to preclude its operational use. However, the PMO must continue to streamline system operations, improve training, and enhance documentation. The system administrators must strictly follow all established security policies and procedures.

Although many measures of effectiveness were successfully met, the OA of DMS 3.0 showed that the system was not sufficiently mature for a full OT&E. Significant improvement was noted in the security posture, based on a limited security assessment. Interfacing to the legacy AUTODIN system was problematic, and especially so within the intelligence community. There were also problems with certificates and Fortezza cards within the Certificate Management Infrastructure.

LESSONS LEARNED

The diversity of site configurations and operational needs poses design and testing challenges. Focus on security training and greater attention to detail during site installation and configuration is necessary and can lead to a relatively secure system. Installing and maintaining DMS is complex, and automated tools for assessing the system security configuration would be helpful. Operational tests have not focused on automated tools because they were under development. We recommend development focus on simplifying and supporting system administrator tasks followed by OT&E events exercising these critical support tasks, tools, and procedures. To achieve DTH closure by September 2003, the intelligence community will need a concerted effort to mature their implementation of DMS with particular focus on their Multi-Function Interpreter and Decision Agent products. Occasionally, DMS messages do not get delivered. In most of these situations, there is some type of system notification to either the sender or to a system administrator. Operational testing needs more focus on how message writers ultimately ensure the messages are received by the intended readers.